(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 November 2003 (20.11.2003)

PCT

(10) International Publication Number
WO 03/096554 A2

(51) International Patent Classification⁷: H04B

(21) International Application Number: PCT/US03/15026

(22) International Filing Date: 13 May 2003 (13.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/378,029 13 May 2002 (13.05.2002) US

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [FR/FR]; 46 Quai A. Le Gallo, F-92648 Boulogne (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **WANG, Charles, Chuanming** [US/US]; 1504 Spearmint Circle, Jamison, PA 18929 (US). **MODY, Sachin, Satish** [IN/US]; 708 White Pine Circle, Lawrenceville, NJ 08648 (US). **ZHANG, Junbiao** [CN/US]; 20 Jenna Drive, Bridgewater, NJ 08807 (US). **RAMASWAMY, Kumar** [IN/US]; 71 Sayre Drive, Princeton, NJ 08540 (US).

(74) Agents: **TRIPOLI, Joseph, S.** et al.; Thomson Licensing, Inc., 2 Independence Way, Suite 2, Princeton, NJ 08543 (US).

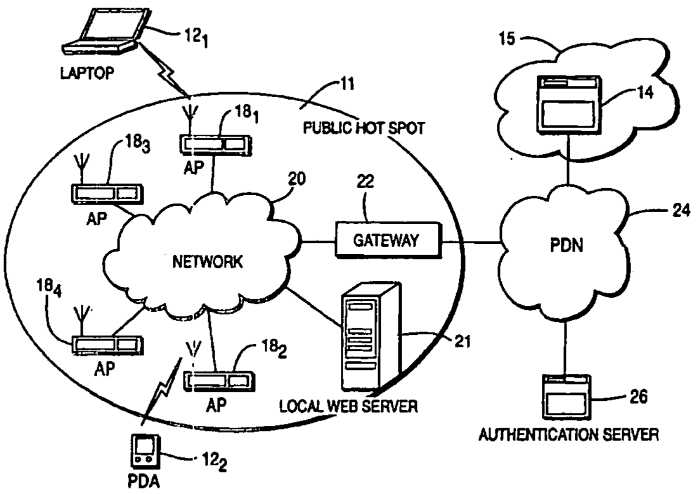
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SEAMLESS PUBLIC WIRELESS LOCAL AREA NETWORK USER AUTHENTICATION



(57) Abstract: A public wireless LAN (11) permits receipt of non-authentication traffic, such as access information requests, from a mobile wireless communications device (121) prior to device authentication by partially opening a controlled port within an access point (181). The wireless LAN re-directs such non-authentication traffic received at the AP from the mobile wireless communications to a local web server (21). The local web server provides reply to the mobile wireless communications device, enabling a determination by the device whether or not to request access. The device seeks access by way of an access request received at the AP. In response, the AP re-directs the access request through an uncontrolled port in the AP to an access server (26) that authenticates device. Upon successful device authentication, the AP fully opens its controlled port to permit the exchange of traffic through that port with the mobile wireless communications device.

WO 03/096554 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SEAMLESS PUBLIC WIRELESS LOCAL AREA NETWORK USER AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This is a non-provisional application claiming the benefit under 35 U.S.C. § 119 of provisional application Serial No. 60/376,029, entitled "SEAMLESS PUBLIC WIRELESS LOCAL AREA NETWORK USER AUTHENTICATION", filed on 13 MAY 2002, which is incorporated by reference herein.

TECHNICAL FIELD

This invention relates to a technique for authenticating a mobile wireless communications device in a public wireless Local Area Network (LAN).

BACKGROUND ART

Advances in the field of wireless LAN technology have resulted in the emergence of publicly accessible wireless LANs (e.g., "hot spots") at rest stops, cafes, libraries and similar public facilities. Presently, public wireless LANs offer mobile wireless communications device users access to a private data network, such as a Corporate Intranet, or a public data network such as the Internet. The relatively low cost to implement and operate a public wireless LAN, as well as the available high bandwidth (usually in excess of 10 Megabits/second) makes the public wireless LAN an ideal access mechanism through which users can exchange packets with an external entity.

When a user travels into a public wireless LAN coverage area, the public wireless LAN first authenticates and authorizes the user prior to granting network access. After authentication, the public wireless LAN Access Point (AP) opens a secure data channel to the mobile wireless communications device to protect the privacy of data exchanged with the device. Presently, many manufacturers of wireless LAN equipment have adopted the IEEE 802.1x protocol for deployed equipment. Hence, the predominant authentication mechanism for wireless LANs utilizes this standard. Unfortunately, the IEEE 802.1x protocol was a safe authentication procedure, but such mechanisms do not permit setting of a Wired Equivalent Privacy (WEP) encryption key in the Web browser. Therefore, data transmitted over wireless LAN after authentication remains unprotected.

Thus, there is need for an authentication process for use in a public wireless LAN environment that permits authentication in accordance with the IEEE 802.1x protocol, thus protecting the privacy of exchanged data, while affording customized interaction mechanisms.

BRIEF SUMMARY OF THE INVENTION

Briefly, in accordance with a preferred embodiment of the present principles, there is provided a method for authenticating the user of a mobile wireless communications device in a public wireless LAN. The method commences upon receipt of a request received from a mobile wireless communications device for non-authentication information, which can include access information, such as the cost of access. In response to such an information request, a controlled port in the public wireless LAN is partially opened to enable transmission of non-authentication (e.g., access) information request through the LAN to a first server that replies with the requested information. Assuming the user of the mobile wireless communications device finds the access terms specified in the reply from the first server acceptable, the user then sends an access request to an authentication server with an authenticating credential. In response to the access request, the authentication server authenticates the user and notifies the public wireless LAN to allow the use of wireless LAN services. Upon successful authentication, the public wireless LAN fully opens the controlled port to permit the exchange of data with the mobile wireless communications device through the controlled port.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 depicts a block schematic diagram of a communications system for practicing the method of the present principles for authenticating the user of a mobile wireless communications device; and

FIGURE 2 depicts a timing chart depicting the sequence of events associated authenticating the user of the mobile wireless communications device in the communications system of FIG. 1.

DETAILED DESCRIPTION

FIGURE 1 depicts a block schematic diagram of a communications network 10 that includes an access arrangement 11 for enabling at least one mobile communication device, and preferably a plurality of mobile communication devices (e.g., mobile communication devices 12_1, and 12_2,) to securely access an external data source 14, which can take the form of a server within a network 15, such as a public data network (e.g., the Internet), or a private data network (e.g., a corporate intranet). In a preferred embodiment, the mobile communication device 12_1 comprises a lap top computer that includes a wireless modem or wireless network access card, whereas the mobile communication device 12_2 comprises a Personal Data Assistant. The access arrangement 11 can also serve other types of mobile wireless communications devices (not shown).

The access arrangement 11 of FIG. 1 includes at least one, and preferably, a plurality of access points (APs), best exemplified by APs 18_1-18_4, via which the mobile wireless communication devices 12_1 and 12_2 can access a public wireless Local Area Network (LAN) 20. Although shown separately, the APs 18_1-18_4 comprise part of the public wireless LAN 20. In the illustrated embodiment, each AP, such as AP 18_1, includes a wireless transceiver (not shown) for exchanging radio frequency signals with a radio transceiver (not shown) within each mobile wireless communication device. To this end, each of the APs 18_1-18_4 employs at least one well-known wireless data exchange protocol, such as the IEEE 802.1x protocol.

The access arrangement 11 also includes a server 21, in the form of a local web server that stores non-authentication information. Such non-authentication information can include access information, such as access terms and conditions, including the cost to the user. The local web server 21 enables a device user to obtain such non-authentication information without the need to establish an actual communications session with the public wireless LAN 20 and thus undergo authentication. Although shown separately, the local web server 21 could reside within the public wireless LAN 20.

A gateway 22 provides a communication path between the public wireless LAN 20 and a packet data network (PDN) 24 that provides a link to the network 15. The PDN 24 thus permits communications between each mobile wireless communications device and the data source 14. The PDN 24 also links the gateway 22 to an authentication server 26. In practice, the authentication server 26 takes the form of a database containing information about potential users to enable authentication of those seeking access to the wireless LAN 20. Rather than exist as a separate stand-alone entity, the authentication server 26 could reside within the public wireless LAN 20. Further, the PDN 24 provides a link between the public wireless LAN 20 and a billing agent (not shown) to facilitate billing device user for accessing the public wireless LAN. As with the authentication server 24, the functionality of the billing agent could reside within the public wireless LAN 20.

In advance of actually establishing an actual authenticated communications session with the public wireless LAN 20, a device user might wish to obtain certain non-authentication information, such as the terms and conditions of access, as well as the cost. Heretofore, the device user could not obtain such non-authentication information from a public wireless LAN whose access points (APs) employ the IEEE 802.1x protocol without establishing an authenticated communications session. The access arrangement 11 of the present principles overcomes this disadvantage by enabling a limited connection with the public wireless LAN 20 to obtain non-authentication information, including access information, prior to actually establishing an authenticated communications session.

FIG. 2 depicts the sequence of interactions that occurs over time among a mobile wireless communication device, say device 12_1, the public wireless LAN 20, the local web server 21, and the authentication server 26 to achieve the desired secure access while permitting receipt of certain information without authentication. Referring to FIG. 2, prior to actually establishing an authenticated communications session, the user of the mobile wireless communications device 12_1 can obtain non-authentication information by first launching an HTTP information request during step 102. The information request is initially received at one of the APs, such as AP 18_1 of FIG. 1. When configured with the IEEE 802.1x protocol, the AP 18_1 of FIG. 1 maintains a controlled port and an un-controlled port through which the AP exchanges information with the mobile wireless communications device 12_1. The controlled port maintained by the AP 18_1 serves as the entryway for non-authentication information to pass through the AP between the public wireless LAN 20 and the mobile wireless communications device 12_1. Ordinarily, the AP 18_1 keeps its controlled port closed in accordance with the IEEE 802.1x protocol until authentication of the mobile wireless communications device. The AP 18_1 always maintains the uncontrolled port open to permit the mobile wireless communications device 12_1 to exchange authentication data with an authentication server, e.g., server 26.

To permit the mobile wireless communications device 12_1 to obtain non-authentication information, and particularly, access information, without authentication in accordance with the present principles, the public wireless LAN 20 causes each AP, such as AP 18_1 of FIG. 1, to partially open its controlled access port after receiving a request for non-authentication information. Partially opening the controlled port in the AP 18_1 enables receipt of such a non-authentication information request in the public wireless LAN 20 through the controlled port during step 104. Upon receipt of the information request, the public wireless LAN 20 redirects the request to the local web server 21 during step 106. Regardless of the destination specified in the information request initially made during step 102, the public wireless LAN 20 always directs the request to the web server 21 of FIG. 1 during step 106. The web server 21 responds to the information request by providing the requested information, (e.g., the access terms and conditions as well as the domain name of the authenticating server 26) to the requesting mobile wireless communications device 12_1 during step 108. Assuming the user of the device finds the terms and condition are acceptable (or the user has negotiated acceptable terms and conditions), the mobile wireless communications device 12_1 transmits to the AP 18_1 an acceptance message during step 110. The acceptance message will identify the authentication server 26 by its name or URL. The mobile wireless device 12_1 will automatically transmit such an acceptance message if the access terms and conditions communicated by the web sever 21 match predefined access criteria stored in the device. In absence of such a match, the user might need to trigger the transmission of an acceptance message.

Upon receiving the acceptance message, the AP 18_1 requests the mobile wireless communications device 12_1 to identify itself during step 112. Assuming the wireless communication device 12_1 employs an Extensible Authentication Protocol (EAP) as is well known in the art, the AP 18_1 will seek identification of the device through an EAP identity request. In response to the EAP identity request, the mobile wireless communications device 12_1 sends an EAP identity response to the AP 18_1 during step 114 for redirection and receipt at the authentication server 26 via the public wireless LAN 20 during step 116.

As part of the process of identifying the device, the public wireless LAN 20 typically checks whether the device user has a relationship with a billing agent serving the wireless LAN 20. If the user has a relationship, then the user need not do anything further as the billing agent will account for the access charges. In the absence of a relationship with a billing agent, the user will need to establish such a relationship. With the user's assent, the wireless LAN 20 can seek to dynamically establish such a relationship.

Upon receipt of the EAP identity response, the AP 18_1 sends the EAP identity response to the authentication server 26 through the uncontrolled port during step 118. The authentication server 26 replies to the EAP identity response by directing an EAP authentication request to the AP 18_1 during step 120 for subsequent transmission via the AP 18_1 to the mobile wireless communications device 12_1 during step 122. The mobile wireless communications device 12_1 replies during step 124 with an EAP authentication response that is received through the uncontrolled port in the AP 18_1. In turn, the AP 18_1 forwards the EAP authentication response to the authentication server 26 during step 126.

Upon successful authentication of the mobile wireless communications device 12_1, the authentication server 26 generates an EAP authentication success message during step 128 for receipt in the AP 18_1. In turn, the AP 18_1 sets an authentication key, typically a Wired Equivalent Privacy (WEP) encryption key, for transmission to the mobile wireless communications device 12_1 during step 130. Lastly, the AP 18_1 fully opens its controlled port to permit an exchange of traffic with the mobile wireless communications device 12_1 through the controlled port.

The foregoing describes a technique for authenticating a mobile wireless communications device in a public wireless LAN that affords the user of the device the opportunity to receive non-authentication information in advance of actually establishing a communications session with the public wireless LAN.

CLAIMS

1. A method for authenticating a mobile wireless communications device in a public wireless Local Area Network (LAN), comprising the steps of:

receiving a request for non-authentication information;

partially opening a controlled port through which the information request is directed to a first server that responds by providing a reply to the mobile wireless communications device;

receiving an access request;

authenticating the mobile wireless communications device through an uncontrolled port; and

fully opening the controlled port to enable the exchange of traffic with the mobile wireless communications device through the controlled port.

2. The method according to claim 1 wherein the request for non-authentication information is directed to the first server irrespective of a destination specified in the request.

3. The method according to claim wherein authenticating step comprises the steps of:

receiving an acceptance from the mobile wireless communications device responsive to the reply to the mobile wireless communications device;

transmitting a user identification request to the mobile wireless communications device;

receiving a user identification response from the mobile wireless communications device in reply to the user identification request; and

re-directing the user identification response to an authentication server.

4. The method according to claim 3 wherein the step of transmitting the user identification request comprises the step of transmitting an Extensible Authentication Protocol (EAP) request.

5. The method according to claim 4 wherein the step of receiving the user identification response comprises the step of receiving an EAP identification response.

6. The method according to claim 1 further comprising the step of setting an authentication key following authentication.

7. The method according to claim 6 wherein the step of setting an authentication key comprises the step of setting a Wired Equivalent Privacy (WEP) encryption key.

8. A communications network for authenticating a mobile wireless communications device, comprising:

a first server for storing non-authentication information;

a second server for authenticating a mobile wireless communications device;

at least one access point (AP) having (a) controlled port via which the AP partially opens in response to a receipt of a request for non-authentication information from a mobile wireless communications device and for directing the information request to the first server which sends a reply for receipt by the mobile wireless communications device, and (b) an uncontrolled port through which the AP directs authentication traffic received from the mobile wireless communications device to the second server which exchanges authentication traffic with the mobile wireless communications device;

a public wireless Local Area Network (LAN) coupled to the one AP and said first and second servers.

9. The system according to claim 8 wherein the AP utilizes a communication protocol in conformance with IEEE 802.1x.

10. The system according to claim 8 wherein the information stored in the first server includes access costs.

11. The system according to claim 8 wherein the second server authenticates the mobile wireless communications device in accordance with an Extensible Authentication Protocol (EAP).

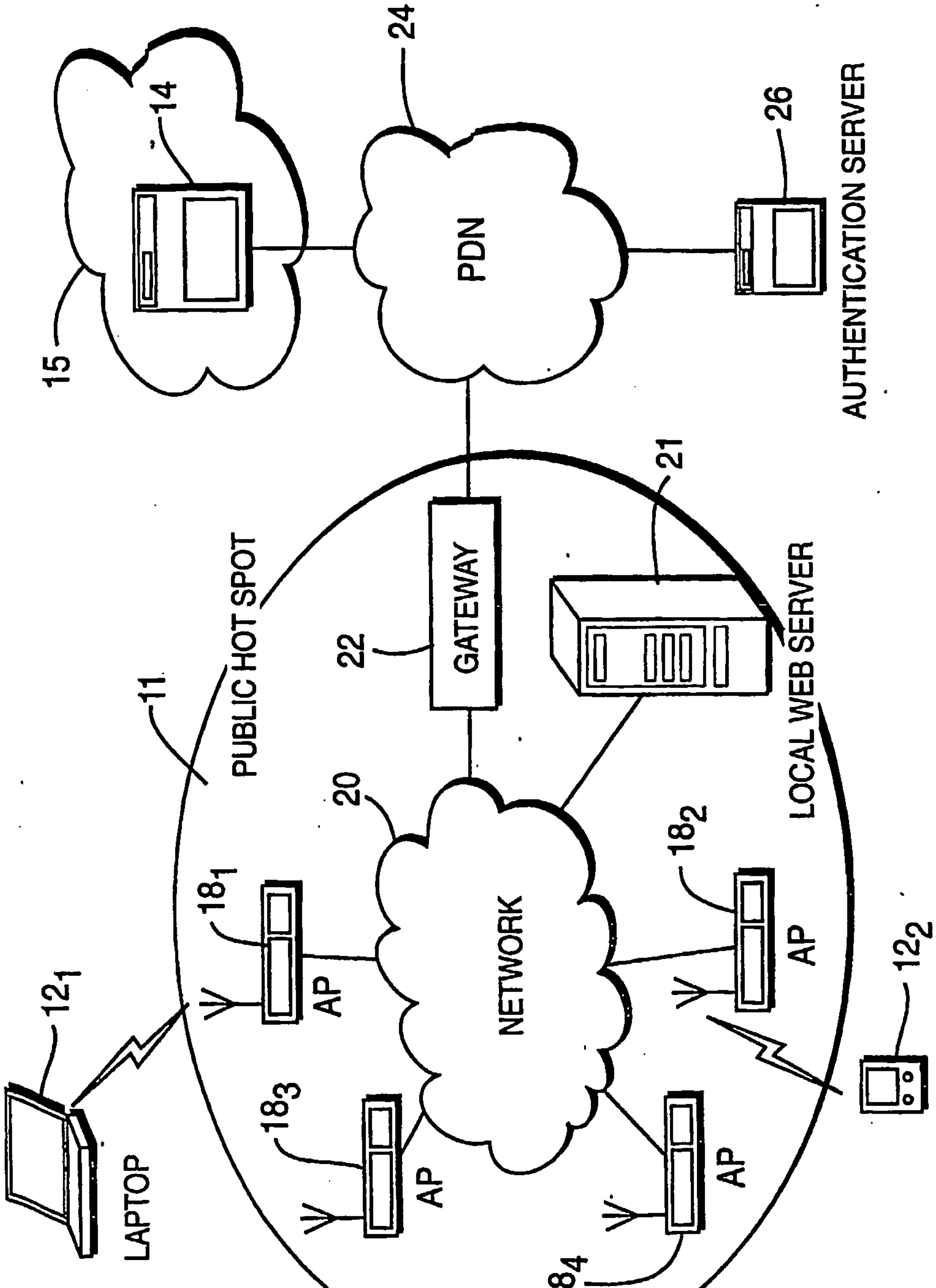
12. The system according to claim 8 wherein the authentication traffic received at the one AP includes an identification of the authentication server.

13. An access point (AP) comprising:

(a) controlled port via which the partially opened in response to a receipt of a request for non-authentication information from a mobile wireless communications device and for directing the information request to a first server which sends a reply for receipt by the mobile wireless communications device, and

(b) an uncontrolled port through which the AP directs authentication traffic received from the mobile wireless communications device to a second server, which exchanges authentication traffic with the mobile wireless communications device.

14. The system according to claim 13 wherein the AP utilizes a communication protocol in conformance with IEEE 802.1x.


15
14
24
PDN
26
AUTHENTICATION SERVER
11
PUBLIC HOT SPOT
22
GATEWAY
21
LOCAL WEB SERVER
20
NETWORK
12_1
LAPTOP
18_1
AP
18_2
AP
18_3
AP
18_4
AP
12_2
PDA

10

FIG. 1

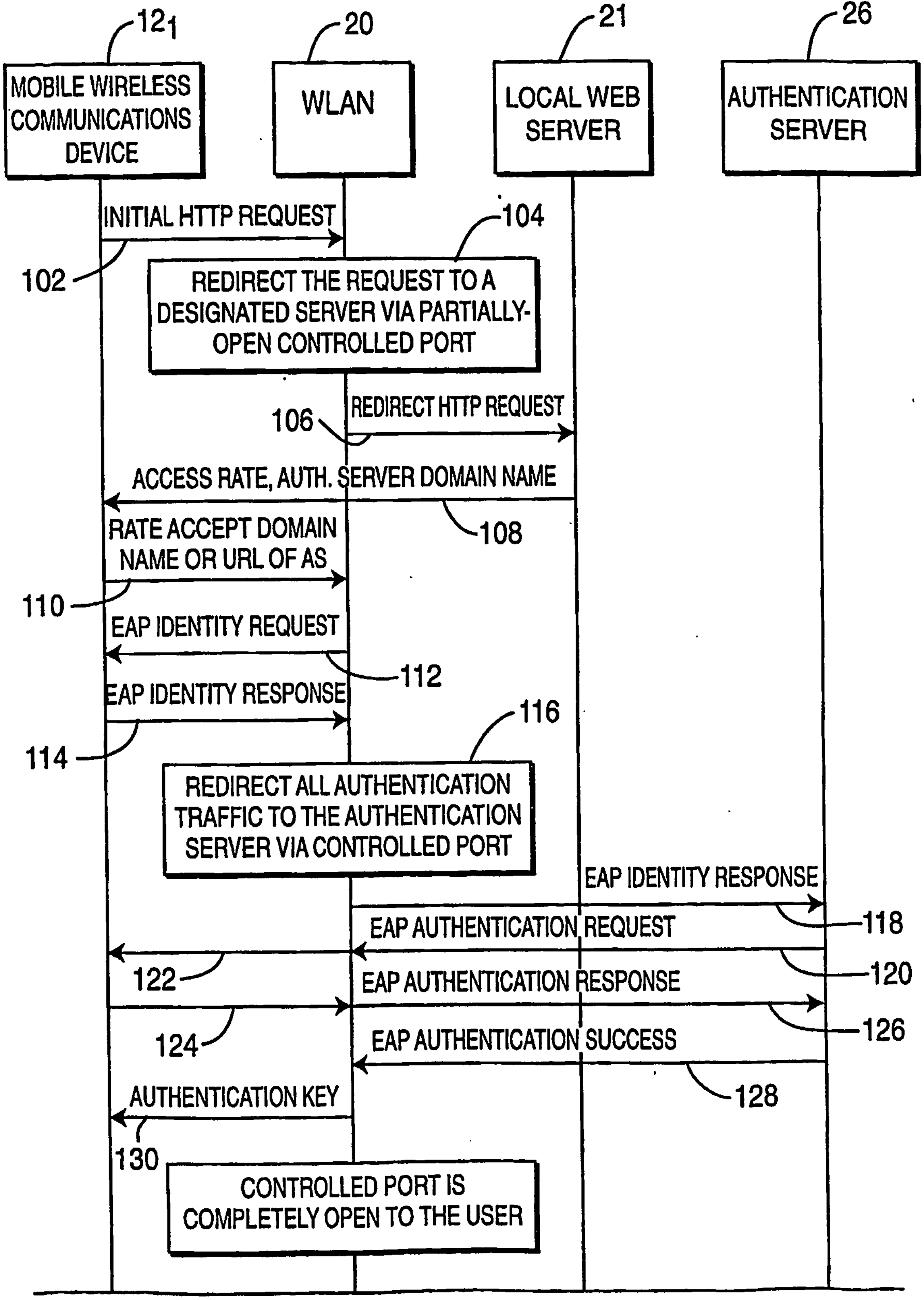

12₁
20
21
26
MOBILE WIRELESS COMMUNICATIONS DEVICE
WLAN
LOCAL WEB SERVER
AUTHENTICATION SERVER
INITIAL HTTP REQUEST
102
104
REDIRECT THE REQUEST TO A DESIGNATED SERVER VIA PARTIALLY-OPEN CONTROLLED PORT
106
REDIRECT HTTP REQUEST
ACCESS RATE, AUTH. SERVER DOMAIN NAME
108
RATE ACCEPT DOMAIN NAME OR URL OF AS
110
EAP IDENTITY REQUEST
112
EAP IDENTITY RESPONSE
114
116
REDIRECT ALL AUTHENTICATION TRAFFIC TO THE AUTHENTICATION SERVER VIA CONTROLLED PORT
EAP IDENTITY RESPONSE
118
EAP AUTHENTICATION REQUEST
120
122
EAP AUTHENTICATION RESPONSE
124
126
EAP AUTHENTICATION SUCCESS
128
AUTHENTICATION KEY
130
CONTROLLED PORT IS COMPLETELY OPEN TO THE USER

FIG. 2